Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Christopher J. Rourk on November 18, 2010

1. (Currently amended) A system of digital data encryption in a digital device, comprising:

generating an inaccurate clock signal that oscillates at different frequencies;

an integrated encryption key generator generating a plurality of encryption keys based upon the input received from an inaccurate timing source; and based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset; ~~at least one key~~ a data buffer; an input/output register that interfaces with memory of the digital device; a control pad coupled to the input/output register; and a memory controller that directs digital data from the memory to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register, wherein the integrated encryption key generator is coupled between the data buffer and the input/output register, and the integrated encryption key generator, the data buffer, the input/output register, the control pad and the memory controller are formed on a single substrate and are accessed through the control pad.

9. (Currently amended) A system configured to decrypt encrypted digital data stored in memory of a digital device, comprising:

generating an inaccurate clock signal that oscillates at different frequencies;

an encryption key generator receiving a signal from an inaccurate clock and generating a plurality of keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset; and for encrypting the encrypted digital data when ~~the encryption key generator~~ the digital device is reset;

a memory controller that generates a memory request to retrieve the encrypted digital data; and

an encryption circuit that decrypts the encrypted digital data in response to the memory request of the memory controller using one or more of the plurality of keys.

12. ***(Currently amended)*** A method of digital data encryption in a digital device, comprising: generating an inaccurate clock signal that oscillates at different frequencies; generating a plurality of keys based on input received from an inaccurate clock, and based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the ~~when~~ digital device is cycled**;** storing the plurality of keys;

placing the digital data in a data buffer; and encrypting the digital data using the at least one of the plurality of keys while the digital data is being placed in a rewritable memory.

22. ***(Currently amended)*** A method to decrypt encrypted digital data stored in memory of a digital device, comprising: generating an inaccurate clock signal that oscillates at different frequencies; generating a plurality of keys based on input received from an inaccurate clock , and based on generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time ~~when~~ the digital device is cycled**;** generating a memory request to retrieve the encrypted digital data; and decrypting the encrypted digital data using one of the plurality of keys.

25. ***(Currently amended)*** A set-top box apparatus in receipt of digital data for storage in a rewritable memory, comprising: generating an inaccurate clock signal that oscillates at different frequencies; an apparatus ~~encryption circuit with at least one key~~ generating a plurality of keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the apparatus is reset; a data buffer filled with the digital data; and a memory controller that directs the storage of the digital data in the rewritable memory with the digital data being encrypted by the encryption circuit and the at least one key after the digital data has entered the data buffer but prior to being stored in the rewritable memory.

Reasons for Allowance

2. The following is an examiner's statement of reasons for allowance: listed below:

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

3. Claims 1-5, 7-15, 17-28 are allowable.

4. Prior art fails to disclose or suggest, "generating an inaccurate clock signal that oscillates at different frequencies", and "generating a plurality of encryption keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset/cycled", and example of prior art that fails to disclose or suggest these limitations is Halpern. Halpern discloses the pseudo random key generator rotates the shift register with every clock pulse. The programmable counter is advanced with every clock pulse. The programmable counter, after producing a carry output, is loaded with the parallel output

from the key generator at the time. The incoming or outgoing real data bits also have an effect on the constellation of the logic interconnections, in that the consecutive data bits are fed with the delay of one complete clock cycle. Halpern discloses the job of the pseudo random data generator, is to provide meaningless data bits to be fed to outlet `d` via the gates when c is high. The gate admits data from the buffer only when c is high. Halpern does not disclose, "generating an inaccurate clock signal that oscillates at different frequencies", and "generating a plurality of encryption keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset/cycled".

5. Prior art fails to disclose or suggest, "generating an inaccurate clock signal that oscillates at different frequencies", and "generating a plurality of encryption keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset/cycled", and example of prior art that fails to disclose or suggest these limitations is Lyle. Lyle discloses the transmitter is implemented so that, after it has entered an initial state determined by the shared secret "Km" and a value "An", and then encrypted a set of data, it is difficult or impossible for an attacker to place the transmitter in the same initial state. One way to accomplish this is to introduce additional randomness into the process by which the transmitter generates the value "An" prior to encrypting data. Introducing a Gaussian analog effect into the pseudo-random function employed to generate "An" would make it more difficult for an attacker to cause the transmitter to generate the same "An" value during both phases of the attack. One way to do this is to incorporate a diode-based white noise source into the "An" value generation process to include such a noise source in "An" value generation circuitry in transmitter. Lyle discloses another way is to require that the transmitter employ an

R-C oscillator, one affected in significant but difficult-to-predict ways by system temperature, voltage, noise, and other physical forces to generate a variable count or time delay during the process of generating the "An" value to include such an oscillator in "An" value generation circuitry in transmitter. Lyle fails to disclose "generating a plurality of encryption keys based on the generated clock signal and a pseudorandom bit pattern generated in a linear feedback shift register each time the digital device is reset/cycled".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

November 18, 2010

/J. E. J./

Examiner, Art Unit 2439